Title	Resilience of airborne networks
Authors(s)	Ahmadi, Hamed, Fontanesi, Gianluca, Katzis, Konstantinos, Shakir, Muhammad Zeeshan, Zhu, Anding
Publication date	2018-09-12
Publication information	Ahmadi, Hamed, Gianluca Fontanesi, Konstantinos Katzis, Muhammad Zeeshan Shakir, and Anding Zhu. “Resilience of Airborne Networks.” Vol. 2018–September. IEEE, 2018.
Conference details	2018 IEEE: IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Bologna, Italy 9-12 September 2018
Publisher	IEEE
Item record/more information	http://hdl.handle.net/10197/10898
Publisher's statement	© 2018 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.
Publisher's version (DOI)	10.1109/PIMRC.2018.8580944

Resilience of airborne networks

Hamed Ahmadi*†, Gianluca Fontanesi*, Konstantinos Katzis‡, Muhammad Zeeshan Shakir§, and Anding Zhu*

* School of Electrical and Electronic Engineering, University College Dublin, Ireland.
† School of Computer Science and Electronic Engineering, University of Essex, UK
‡ Department of Computer Science and Engineering, European University Cyprus, Cyprus
§ School of Engineering and Computing, University of the West of Scotland, Paisley, Scotland, UK

***Abstract*—Networked flying platforms can be used to provide cellular coverage and capacity. Given that 5G and beyond networks are expected to be always available and highly reliable, resilience and reliability of these networks must be investigated. This paper introduces the specific features of airborne networks that influence their resilience. We then discuss how machine learning and blockchain technologies can enhance the resilience of networked flying platforms.**

***Index Terms*—Networked flying platforms, resilience, self-organizing networks, machine learning, blockchain**

I. INTRODUCTION

Unmanned Aerial Vehicles (UAVs) introduced a new challenge to cellular networks by acting as flying User Equipments (UEs) that have much higher elevation than ground users. In Fifth Generation (5G) and beyond networks UAVs will be used for providing network services to ground and flying UEs. In [1], we introduced an architecture for Network Flying Platform (NFP) in 5G and beyond networks. In this work, we aim to introduce and investigate the issues related to the resilience of airborne networks and in particular the introduced NFPs.

II. NETWORK RESILIENCE

In the literature there are several definitions for resilience of networks. In [2] resilience is defined as the capability if the network to recover from the failures. Sterbenz et al in [3] define resilience as the ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation. According to [3] resilience disciplines are classified into two classes of challenge tolerance and trustworthiness related disciplines. The first class relate to the design of the system and include survivability, disruption tolerance and traffic tolerance. The class of trustworthiness disciplines relate to system performance and include dependability, security and performability. In studying the resilience of airborne networks, we follow the definition provided by [3] and consider all the mentioned disciplines. However, due to the special case of airborne networks we need to emphasize on some of the disciplines and add new ones. This is mainly because [3] focuses on fixed networks and misses the features of wireless like multi-operator environments and spectrum/infrastructure sharing.

III. NFP FEATURES AFFECTING THE RESILIENCE

Talking about resilience of each type of networks, we have to consider its and its components specifications and limitations. NFPs have unique features that affect their resilience.

A. Mobility

In an NFP, e.g. 3-layer architecture in [1], all the High Altitude Platforms (HAPs), Medium Altitude Platforms (MAPs) and Low Altitude Platforms (LAPs) are not fixed and have the ability to change their position and possibly their altitude. In one hand, mobility introduces challenges like possible collisions among the flying platforms, backhaul challenges, and connection loss. On the other hand, mobility enables the network to proactively respond to unpredicted events like UAV failures or a sudden appearance of a demand hotspot. In the first scenario, the platforms especially LAPs can re-organise to preform self-healing, while in the second scenario an LAP can move closer to the demand hotspot reducing the distance between the access point and UEs and the other LAPs reshape to cover the rest of the area. Although mobility is not considered in [3] classification, it will have a significant influence on challenge tolerance related disciplines like distribution tolerance and traffic tolerance as can be seen in the examples above.

B. Energy limitations

Most of the existing work [1], [4] consider battery powered UAVs as the LAPs. This means that the UAVs have a limited operation time and need to fly to charging stations imposing a (predictable) disruption to the network. This feature clearly illustrates the importance of reliable self-organising mechanisms in the network. In these scenarios the self-organising system can either seamlessly replace the leaving UAV with another UAV (redundant), or change the network parameters, including the position of LAPs, to deal with this disruption.

C. Physical vulnerabilities

Flying platforms are physically more vulnerable to accidental and intentional disruptions than fixed networks components. Accidents that can take LAPs down include lightning, strong wind, and clashing with birds. Flying platforms can also be targets of intentional disruptions like shooting or spoofing. Moreover, intruding drones pretending to be members of NFP can disrupt the network functionality without causing problem to a single platform.

D. Multi-operator environment

Open air is not a restricted area, except restricted zones defined by authorities, and several NFP operators

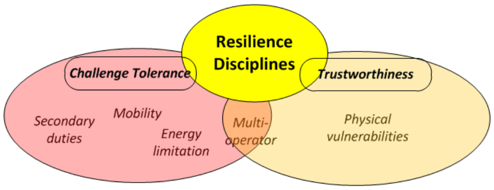

Fig. 1: Classification of NFP features

and other professional/amateur drone operators can co-exist. This dynamic environment will increase the chance of collisions, turbulences, interference, and line-of-sight blockage which affects both challenge tolerance and trustworthiness related features of the network.

E. secondary duties

According to design and need of the system flying platforms specially LAPs and MAPs can have secondary duties like surveillance or protecting the network by spoofing intruding UAVs [4]. Similar to energy limitation case, this may cause the UAVs to leave their network duties. Unlike the battery recharging case, the secondary duties are not always predictable, especially in the case of intrusion protection, which makes providing a redundant UAV to seamlessly take on network duties of the leaving UAV more challenging. In these scenarios self-healing mechanisms help the network to maintain its Quality of Service (QoS). Figure 1 shows the classification of aforementioned features.

IV. Strategies to enhance resilience of NFPs

Most of the aforementioned features of NFPs that influence their resilience are classified as challenge tolerance-related which are not measurable. The challenges related to these features should be addressed in the design and engineering of the network. Although the resilience of a network cannot be measured based on its design and engineering, they effect dependability, security and performability of networks which are measurable.

The dynamic environment and the duties of NFPs require an architecture that enables autonomous reactions to different disruptions. Therefore, NFP can benefit from Self-organising Network (SON) technologies. As defined in [5], SONs are adaptive, autonomous, and they are able to independently decide when or how to trigger certain actions based on interaction with the environment. In [1] we proposed a multi-layer architecture for NFPs and studied NFP specific SON features. To achieve better resilience for NFPs we can use machine learning and blockchain technologies.

A. Machine learning

A survey of machine learning techniques used in SON for wireless networks and their applications is provided in [5]. To the best of our knowledge there is no existing work that studies the application of *machine learning* in self-organizing airborne networks.

Resilinet project [3] proposes a two-phase resilience strategy where the first phase is responsible for dealing with the disruption and maintaining an acceptable level of service while the second phase aims to help the system to evolve and prevent and/or prepare for similar future disruptions. Phase one consists of detect, defend, remediate and recover, and phase two has two activities of diagnose and refine. A resilient airborne network can quickly detect disruptions and remediate. However, an NFP can be more resilient using carefully trained learning algorithms that can predict disruptions like battery limitation or even possible intrusions.

Optimization and game theoretic modeling are the most common methods in the existing works [1] for planing the movement and position of flying platforms to maximize the coverage area or to maximize the delivered data rate to UEs. Several parameters effecting the decision of these algorithms which are traditionally set to an empirical mean value or inaccurately chosen can be learnt by machine learning algorithms based on the previous experiences [6]. This leads to faster and more accurate reaction to a disruption.

B. Blockchain and smart contracts

Blockchain can be defined as a resilient, reliable, transparent and decentralized way of storing and distributing a database across all nodes of a network [7]. Blockchain can assist with the security of NFPs against intruders pretending to be members of the network and/or spoofing attempts.

In a multi-operator environment smart contracts can significantly help to manage space and spectrum sharing. A smart contract is basically a contract that its terms are enforced and executed automatically as computer codes among the participating entities without the need of an en-forcer or a third party. Smart contracts can facilitate deployment of automated charging stations at the roof of the building reducing the flight distance and time of UAVs to recharge their batteries.

V. Conclusions

In this paper we introduced specific features of NFPs that affect their resilience. Most of these features are related to the design and engineering of the network, and are not easily measurable. We also named machine learning and blockchain as two promising technologies that can improve resilience of airborne networks.

References

[1] H. Ahmadi *et al.*, "A novel airborne self-organising architecture for 5g+ networks," in *IEEE VTC2017-Fall*, Sept 2017, pp. 1–5.

[2] N. Alliance, "5g white paper," *Next generation mobile networks, white paper*, pp. 1–125, 2015.

[3] J. P. Sterbenz *et al.*, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," *Comput. Net.*, vol. 54, no. 8, pp. 1245–1265, 2010.

[4] S. A. R. Naqvi *et al.*, "Drone-aided communication as a key enabler for 5g and resilient public safety networks," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 36–42, 2018.

[5] P. Valente Klaine *et al.*, "A survey of machine learning techniques applied to self organizing cellular networks," *IEEE Commun. Surv. & Tut.*, 2017.

[6] A. Silver. 3 ways nokia is using machine learning in 5G networks. [Online]. Available: https://spectrum.ieee.org/tech-talk/telecom/wireless/3-ways-nokia-is-using-machine-learning-in-5g-networks

[7] A. Malki and M. Weiss, "Automating ex-post enforcement for spectrum sharing: A new application for block-chain technology," 2016.